Códigos de convolución desde el punto de vista de teoría de control. Análisis de la observabilidad

M. Isabel GARCÍA-PLANAS[#1], Sonia TARRAGONA[*2], Laurence E. Um[#3]

[1]Departament de Matemàtica Aplicada I, Universitat Politècnica de Catalunya
Diagonal 647, 08038 Barcelona, España

[1]maria.isabel.garcia@upc.edu

[2]Departamento de Matemáticas, Universidad de León
Campus de Vegazana s/n, 24071 León, España

[2]sonia.tarragona@unileon.es

[3]Université Mohammed V.
Laboratoire de Recherche Mathématiques, Informatique et Applications
Avenue des Nations Unies, Agdal, BP: 554, Rabat, Marruecos

[3]laurainlee@yahoo.fr

Resumen— **En este trabajo se realiza un estudio detallado de la estructura algebraica de los códigos de convolución empleando técnicas de la teoría de sistemas lineales. La conexión entre estos conceptos ayuda a comprender mejor las propiedades de los códigos convolucionales. Más explícitamente, esta conexión es debida a que los conceptos de controlabilidad y observabilidad, de los sistemas lineales, pueden ser expresados, en el marco de los códigos convolucionales, como el carácter no catastrófico de los códigos. En particular, en este trabajo se examina la propiedad de "output-observabilidad" y damos condiciones que aseguran el cumplimiento de esta propiedad.**

Clave— **Códigos, sistemas lineales, output-observabilidad.**

I. INTRODUCCIÓN

En su origen, la teoría de códigos se ha dedicado, principalmente, a la teoría de la información. La teoría de códigos, de hecho, surgió de la necesidad de una mejor comunicación y un mejor almacenamiento de datos informáticos.

En concreto, los códigos convolucionales se utilizan para proteger la información añadiendo redundancia a la misma, y en muchas ocasiones, para transferir datos con altas exigencias de velocidad. Para este fin se requieren códigos potentes y con tasas elevadas. Estos códigos están frecuentemente implementados en composición con un código de difícil decisión, particularmente de Reed Solomon.

Los códigos convolucionales más utilizados son los binarios y son una alternativa a los códigos de bloque por su simplicidad de generación y por su un pequeño registro de desplazamiento.

Los códigos convolucionales fueron introducidos por Elias [5], quien planteó el uso de una matriz polinomial, $G(z)$, en el proceso de codificación. De esta forma se consigue la generación de la línea de código sin usar espacio de memoria anterior.

G. D Forney en {7} explica que el término "convolucional" se utiliza porque las secuencias de salida pueden considerarse como la convolución de la secuencia de entrada con las secuencias en el codificador.

Un punto fundamental en la teoría de códigos convolucionales fue encontrar un método para la construcción de códigos de una determinada tasa y complejidad con buena discrepancia acumulada (distancia libre). Diversos métodos han sido introducidos con este fin. Y, es por ello, que existe una cantidad considerable de publicaciones en el tema que nos ocupa: la teoría de códigos convolucionales sobre cuerpos finitos

(ver, por ejemplo, [5,6,10,11,13,14,16,17, 20]).

Es bien conocida la relación entre códigos convolucionales y la teoría de sistemas lineales sobre cuerpos finitos.

Así, una descripción de códigos convolucionales puede ser dada mediante un sistema lineal discreto invariante en el tiempo (ver [17,19,20]). Queremos hacer notar que la teoría de sistemas lineales es bastante general y que permite todo tipo de ejes discretos de tiempo y espacios de señales.

El objetivo de este trabajo es analizar las propiedades de los códigos convolucionales con la ayuda de las herramientas de la teoría de sistemas. Se presenta una representación entrada-salida de un código convolucional, y se caracterizan los sistemas “output-observables”. La “output-observabilidad” permite la posibilidad de describir los estados simplemente conociendo las salidas. En este artículo se presenta un sencillo test para determinar la “output-observabilidad" de un sistema.

En el caso de los sistemas lineales con coeficientes en el cuerpo de los números reales o complejos el problema de control ha sido ampliamente estudiado (véase [3,8,9], por ejemplo). Este problema para sistemas de control sobre los anillos conmutativos también ha sido estudiado (ver [15] por ejemplo). Para la teoría de códigos convolucionales, Rosenthal [18] presentó un primer paso hacia un algoritmo algebraico de decodificación. Se basa en una descripción entrada/estado/salida del código ligado a la matriz de controlabilidad, que es la matriz de comprobación de paridad de un código de bloque algebraicamente decodificable. Más recientemente, otros autores también estudian la teoría de códigos convolucionales utilizando las herramientas de la teoría de control [1,2,12,21].

II. PRELIMINARES

En esta sección, presentamos algunas nociones básicas sobre la teoría de códigos.

Sea $\mathcal{A} = \{a_1, \ldots, a_q\}$ un conjunto finito de símbolos, llamado alfabeto de los mensajes. Denotamos por $\mathcal{M}$ al conjunto de todas las sucesiones de símbolos en $\mathcal{A}$ de longitud k. También denotamos por $\mathcal{R}$ al conjunto de todas las sucesiones de símbolos en $\mathcal{A}$ de longitud n. Consideramos k y n enteros positivos y $k \leq n$.

Estamos interesados en el caso en que $\mathcal{A} = \mathbb{F}_q$ es un cuerpo finito conmutativo de q elementos.

Consideremos $f : \mathcal{A} \longrightarrow \mathcal{A}^*$ donde $\mathcal{A}^* = \bigcup_{n\geq 0} \mathcal{A}^n$ y $\mathcal{A}^n = \mathcal{A} \times \ldots \times \mathcal{A}$. Un código está definido como la imagen $f(\mathcal{A}^n) = C \subseteq \mathcal{A}^*$.

Destacamos los siguientes conceptos:

- Operador traslación por la izquierda σ y operador traslación por la derecha σ^{-1} sobre la secuencia de espacios $\mathcal{A}^*$ definidos como se sigue:

$$\sigma(a_0, a_1, a_2, \ldots) = (a_1, a_2, a_3, \ldots),$$
$$\sigma^{-1}(a_0, a_1, a_2, \ldots) = (0, a_0, a_1, a_2, \ldots),$$

- $C \subseteq \mathcal{A}^*$ se dice que es invariante por el operador traslación por la derecha (izquierda) cuando $\sigma^{-1}C \subseteq C$ ($\sigma C \subseteq C$).

- Si para cada elemento de C existe un número finito de elementos no nulos, se dice que C es compacto.

Definición 1

Un código corrector de errores $C \subseteq \mathcal{A}^*$ se dice que es un código convolucional, si C es lineal (considerado como un espacio vectorial sobre $\mathbb{F}_q$ con la suma usual de vectores), invariante por el operador traslación por la derecha y tiene soporte compacto.

Siguiendo los trabajos de Rosenthal y York \cite{RY}, un código convolucional está definido como un submodulo de $\mathbb{F}^n[s]$.

Definición 2

Sea $C \subseteq \mathcal{A}^*$un código. Entonces C es un código convolucional si y sólo si Ces un $\mathbb{F}[s]$-submodulo de $\mathbb{F}^n[s]$.

Corolario 1

Existe un morfismo de módulos inyectivo.

$$\begin{aligned} \psi : \mathbb{F}^k[s] &\longrightarrow \mathbb{F}^n[s] \\ u(s) &\longrightarrow v(s). \end{aligned}$$

Equivalentemente, existe una matriz polinomial $G(s)$ (llamada codificador) de orden $n \times k$ de rango maximal tal que

$$C = \{v(s) \mid \exists u(s) \in \mathbb{F}^k[s] : v(s) = G(s)u(s)\}.$$

La tasa de codificación k/n es conocida como la ratio o proporción de un código convolucional.

Denotamos por ν_i al máximo de todos los grados de cada uno de los polinomios de cada línea.

Definimos la complejidad del codificador como $\delta = \sum_{i=1}^n \nu_i$. Y, finalmente, se define la complejidad del código de convolución $\delta(C)$ como el máximo de todos los grados de los mayores menores de $G(s)$.

Ejemplo 1 Consideremos el mensaje $u(s) = (1 \quad 1 \quad 0 \quad 1 \quad 1) = 1 + s + s^3 + s^4$ y $g_1 = 1 + s + s^2$ $g_2 = 1 + s^2$ los polinomios generadores de $G(s)$, entonces el mensaje codificado es

$$v(s) = G(s)u(s) = \begin{pmatrix} 1 + s + s^2 \\ a + s^2 \end{pmatrix} (1 + s + s^3 + s^4) = \begin{pmatrix} 1 + s^6 \\ 1 + s + s^2 + s^4 + s^5 + s^6 \end{pmatrix}.$$

La representación de un código mediante una matriz polinomial no es única, pero tenemos la siguiente proposición.

Proposición 1

Dos $n \times k$ *codificadores racionales* $G_1(s)$, $G_2(s)$ *definen el mismo código convolucional, si y sólo si existe una* $k \times k$ *matriz unimodular* $U(s)$ *tal que* $G_1(s)U(s) = G_2(s)$.

Después de una adecuada permutación de las filas, se puede suponer que la matriz generador $G(s)$ es de la forma

$$G(s) = \begin{pmatrix} P(s) \\ Q(s) \end{pmatrix}$$

donde $P(s) \in \mathbb{F}^{(n-k)\times k}$ y $Q(s) \in \mathbb{F}^{k\times k}$ son factores coprimos.

Es posible considerar codificadores racionales equivalentes

$$\begin{pmatrix} P(s) \\ Q(s) \end{pmatrix} Q^{-1}(s) = \begin{pmatrix} P(s)Q^{-1}(s) \\ I \end{pmatrix}.$$

A. Sistemas y Códigos

Un sistema dinámico es un modelo de un fragmento aislado de la naturaleza con un entorno dinámico que puede ser observado y estudiado:

Este comportamiento es la respuesta del sistema a un estímulo externo, y esta respuesta puede no ser siempre la misma, sino que depende también de las circunstancias actuales del sistema dinámico.

En otras palabras, un sistema dinámico es un proceso que tiene una magnitud que varía con el tiempo según una ley determinística o estocástica.

Más específicamente:

Definición 3

Un sistema lineal discreto invariante en el tiempo se describe mediante las ecuaciones:

$$\left.\begin{aligned} x(t+1) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t) + Du(t) \end{aligned}\right\} \qquad (1)$$

donde $A \in M_{\delta}(\mathbb{F})$, $B \in M_{\delta\times k}(\mathbb{F})$, $C \in M_{(n-k)\times\delta}(\mathbb{F})$, $D \in M_{(n-k)\times k}(\mathbb{F})$ *son matrices constantes sobre el cuerpo* $\mathbb{F}$, *y* $u(t) \in \mathbb{F}^k$, $x(t) \in \mathbb{F}^{\delta}$, $y(t) \in \mathbb{F}^p$ *son los vectores de las entradas, de los estados y de las salidas, respectivamente*.

Por simplicidad, y si no hay confusión posible, escribiremos simplemente $p = n - k$. También, por simplificar, denotaremos los sistemas por cuaternas de matrices (A, B, C, D).

Una solución del sistema (1) puede ser obtenida haciendo uso de la transformada de Laplace.

Sean $u(s)$, $x(s)$, $y(s)$ las transformadas de Laplace de las variables u, x, y de un sistema lineal invariante en el tiempo. Entonces aplicando la transformada de Laplace a las ecuaciones del sistema (1), tenemos

$$\left.\begin{aligned} sx(s) &= Ax(s) + Bu(s) \\ y(s) &= Cx(s) + Du(s) \end{aligned}\right\} \qquad (1)$$

y como resultado tenemos

$$y(s) = (C(sI - A)^{-1}B + D)u(s), \qquad (1)$$

llamada la función de transferencia del sistema y

$$C(sI - A)^{-1}B + D$$

la matriz de transferencia.

La formulación de la función de transferencia del sistema no da información sobre el comportamiento en el interior del sistema, tal es el caso de los modos inestables no observables. Por lo tanto, la matriz de transferencia no puede ser usada para estudiar las propiedades de control de un sistema con estas características. La descripción de entrada-salida permite estudiar las propiedades sobre control de un sistema dinámico.

Definición 4

Sea $H(s)$ *una matriz racional. Si* $H(s)$ *es la matriz de transferencia de un sistema* (A, B, C, D) *entonces* (A, B, C, D) *es llamado una realización del sistema*.

A partir de este momento consideraremos una realización (A, B, C, D) de la matriz racional $P(s)Q^{-1}(s)$ obtenida a partir de la matriz de codificación $G(s)$.

Ejemplo 2 Sea $G(s)$ la matriz de codificación del ejemplo 1

$$G(s) = \begin{pmatrix} 1 + s + s^2 \\ 1 + s^2 \end{pmatrix} = \begin{pmatrix} P(s) \\ Q(s) \end{pmatrix}$$

Luego,

$$C(sI - A)^{-1}B + D = P(s)Q(s)^{-1} = 1 + \frac{s}{1 + s^2}$$

Obtención de las matrices A, B, C y D:

$D = 1$,

Si

$$C(sI - A)^{-1}B = \frac{c_0 + c_1 s}{a_0 + a_1 s + s^2}$$

entonces

$$A = \begin{pmatrix} -a_1 & -a_0 \\ 1 & 0 \end{pmatrix},\ B = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

$$C = (c_1 \quad c_0)$$

Luego,

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ C = (1 \quad 0).$$

III. "OUTPUT-OBSERVABILIDAD"

Relacionado con la realización minimal de un codificador es la propiedad de "output-observabilidad".

Definición 5

El sistema (A,B,C,D) se dice que es "output-observa ble" si la secuencia de estados $x(0),\dots,x(\ell)$ está unívo-camente determinada por el conocimiento de la suce- sión de salidas $y(0),\dots,y(\ell)$ mediante un número finito de pasos $\ell \in \mathbf{N}$.

Observar que $x(1),\dots,x(\ell)$ están determinados mediante el conocimiento de $x(0)$ and $u(0),\dots,u(\ell-1)$ debido a que

$$
\begin{aligned}
x(1) &= Ax(0) + Bu(0)\\
x(2) &= Ax(1) + Bu(1) =\\
&= A^2x(0) + ABu(0) + Bu(1)\\
&\vdots\\
x(\ell) &= Ax(\ell-1) + Bu(\ell-1) =\\
&= A^\ell x(0) + A^{\ell-1}Bu(0) + \dots +\\
&\quad +ABu(\ell-2) + Bu(\ell-1),
\end{aligned}
$$

y los elementos $x(0)$, y $u(0),\dots,u(\ell-1)$ pueden ser obtenidos resolviendo el siguiente sistema matricial de ecuaciones (4).

$$
\begin{aligned}
y(0) &= Cx(0) + Du(0)\\
y(1) &= Cx(1) + Du(1) =\\
&= CAx(0) + CBu(0) + Du(1)\\
&\vdots\\
y(\ell) &= Cx(\ell) + Du(\ell) =\\
&= CA^\ell x(0) + CA^{\ell-1}Bu(0) + \dots +\\
&\quad +CBu(\ell-1) + Du(\ell)
\end{aligned}
\tag{1}
$$

que podemos describir de forma matricial de la manera

$$
\begin{pmatrix}
C & D & & & & \\
CA & CB & D & & & \\
CA^2 & CAB & CB & D & & \\
\vdots & & \ddots & \ddots & & \\
CA^\ell & CA^{\ell-1}B & CA^{\ell-2}B & \dots & CB & D
\end{pmatrix}
\begin{pmatrix} x(0)\\ u(0)\\ \vdots\\ u(\ell)\end{pmatrix}
=
\begin{pmatrix} y(0)\\ y(1)\\ \vdots\\ y(\ell)\end{pmatrix}
$$

Llamaremos $T_\ell(A,B,C,D)$ (que simplemente escribiremos T_ℓ si no hay posibilidad de confusión) a la matriz

$$
T_\ell =
\begin{pmatrix}
C & D & & & & \\
CA & CB & D & & & \\
CA^2 & CAB & CB & D & & \\
\vdots & & \ddots & \ddots & & \\
CA^\ell & CA^{\ell-1}B & CA^{\ell-2}B & \dots & CB & D
\end{pmatrix}
$$

Tenemos la siguiente proposición.

Proposición 2

Un sistema (A,B,C,D) es "output-observable" si y sólo si la matriz T_ℓ tiene rango máximo para todo $\ell \in \mathbf{N}$.

Demostración:

En primer lugar, se observa que para cada ℓ, la matriz T_ℓ es la matriz correspondiente al sistema (4). Luego, si el número de filas es mayor que el número de columnas, hay valores de $y(0),\dots,y(\ell)$ para los cuales el sistema no tiene solución. Por lo tanto, supondremos que el número de filas es menor o igual que el número de columnas. Es bien sabido que en este caso y para cada ℓ, los sistemas (4) tiene solución para todo $y(0),\dots,y(\ell)$ si y sólo si los sistemas tienen rango máximo. □

Sea (A,B,C,D) un sistema y consideremos las matrices que escribiremos $M_\ell(A,B,C,D)$ (y que si no hay confusión posible, simplemente escribiremos M_ℓ) definidas de la siguiente manera:

$$
M_\ell =
\begin{pmatrix}
A & B & -I & 0 & 0 & 0 & \dots & & 0 & 0\\
C & D & 0 & 0 & 0 & 0 & & & & \\
0 & 0 & A & B & -I & 0 & & & & \\
0 & 0 & C & D & 0 & 0 & & & & \\
\vdots & & & & & \ddots & & & & \\
 & & & \dots & & & & A & B & -I & 0\\
 & & & \dots & & & & C & D & 0 & 0\\
 & & & \dots & & & & 0 & 0 & C & D
\end{pmatrix}
\in M_{(\ell(\delta+p)+p)\times(\ell+a)(\delta+k)}(\mathbb{F}).
$$

Tenemos el siguiente resultado.

Teorema 1

Sea (A,B,C,D) un sistema. Entonces

$$\operatorname{rango} T_\ell + \ell\delta = \operatorname{rango} M_\ell.$$

Demostración:

Haciendo transformaciones elementales por bloques fila y bloques columna, tenemos

$$\operatorname{rango}\begin{pmatrix} A & B & -I & 0 & 0 & 0 & \dots & & 0 & 0\\ C & D & 0 & 0 & 0 & 0 & & & & \\ 0 & 0 & A & B & -I & 0 & & & & \\ 0 & 0 & C & D & 0 & 0 & & & & \\ \vdots & & & & & \ddots & & & & \\ & & & \dots & & & & A & B & -I & 0\\ & & & \dots & & & & C & D & 0 & 0\\ & & & \dots & & & & 0 & 0 & C & D \end{pmatrix} =$$

$$\operatorname{rango}\begin{pmatrix} I & & & & & & & \\ & \ddots & & & & & & \\ & & I & & & & & \\ & & & C & D & & & \\ & & & CA & CB & D & & \\ & & & CA^2 & CAB & CB & D & \\ & & & \vdots & & \ddots & & \\ & & & CA^\ell & CA^{\ell-1}B & & CB & D \end{pmatrix}$$

□

Con el fin de obtener propiedades, definimos la siguiente relación de equivalencia que preserva las propiedades requeridas.

Definición 6

Los sistemas (A,B,C,D) y (A_1,B_1,C_1,D_1) *son feedback equivalentes, que escribiremos*

$$(A,B,C,D) \sim (A_1,B_1,C_1,D_1),$$

si y sólo si

$$\begin{pmatrix} A_1 & B_1\\ C_1 & D_1\end{pmatrix} = \begin{pmatrix} P^{-1} & W\\ 0 & S\end{pmatrix}\begin{pmatrix} A & B\\ C & D\end{pmatrix}\begin{pmatrix} P & 0\\ V & R\end{pmatrix},$$

para ciertas matrices $P \in M_\delta(\mathbb{F})$, $R \in M_k(\mathbb{F})$, $S \in M_p(\mathbb{F})$, $V \in M_{k\times\delta}(\mathbb{F})$ y $W \in M_{\delta\times p}(\mathbb{F})$.

Observación 1

Esta relación de equivalencia generaliza la relación de equivalencia de semejanza:

$$(A,B,C,D) \simeq (A_1,B_1,C_1,D_1)$$

si y sólo si:

$$(A_1,B_1,C_1,D_1) = (P^{-1}AP, P^{-1}B, CP, D)$$

Es suficiente considerar $V=0$, $W=0$, $R=I_m$, $S=I_p$.

Proposición 3

Sean (A,B,C,D) y (A_1,B_1,C_1,D_1) *dos sistemas equivalentes bajo la relación de equivalencia considerada. Entonces* $\operatorname{rango} M_\ell(A,B,C,D) = \operatorname{rango} M_\ell(A_1,B_1,C_1,D_1)$, *para todo* $\ell \in \mathbf{N}$.

Demostración:

Llamando

$$\mathbf{P} = \begin{pmatrix} P^{-1} & W & & & & & & \\ 0 & S & & & & & & \\ 0 & 0 & P^{-1} & W & & & & \\ 0 & 0 & 0 & S & & & & \\ & & & & \ddots & & & \\ & & & & & P^{-1} & W & \\ & & & & & 0 & S & \\ & & & & & & & S \end{pmatrix}$$

y

$$\mathbf{Q} = \begin{pmatrix} P & 0 & & & & & & & \\ V & R & & & & & & & \\ & & P & 0 & & & & & \\ & & V & R & & & & & \\ & & & & \ddots & & & & \\ & & & & & P & 0 & & \\ & & & & & V & R & & \\ & & & & & & & R & \\ & & & & & & & & R \end{pmatrix}$$

$$
\mathbf{P}\begin{pmatrix}
A & B & -I & 0 & 0 & 0 & \dots & & 0 & 0\\
C & D & 0 & 0 & 0 & 0 & & & & \\
0 & 0 & A & B & -I & 0 & & & & \\
0 & 0 & C & D & 0 & 0 & & & & \\
\vdots & & & & & \ddots & & & & \\
 & & & \dots & & & A & B & -I & 0\\
 & & & \dots & & & C & D & 0 & 0\\
 & & & \dots & & & 0 & 0 & C & D
\end{pmatrix}\mathbf{Q} =
$$

$$
\begin{pmatrix}
A_1 & B_1 & -I & 0 & 0 & 0 & \dots & & 0 & 0\\
C_1 & D_1 & 0 & 0 & 0 & 0 & & & & \\
0 & 0 & A_1 & B_1 & -I & 0 & & & & \\
0 & 0 & C_1 & D1 & 0 & 0 & & & & \\
\vdots & & & & & \ddots & & & & \\
 & & & \dots & & & A_1 & B_1 & -I & 0\\
 & & & \dots & & & C_1 & D_1 & 0 & 0\\
 & & & \dots & & & 0 & 0 & C_1 & D1
\end{pmatrix}.
$$

Entonces, ambas matrices tienen el mismo rango. □

Corolario 2

Sean (A,B,C,D), *y* (A_1,B_1,C_1,D_1) *dos sistemas equiva-lentes bajo la relación de equivalencia considerada. Entonces*

$$\operatorname{rango} T_\ell(A,B,C,D) = \operatorname{rango} T_\ell(A_1,B_1,C_1,D_1),$$

para todo $\ell \in \mathbf{N}$.

IV. TEST PARA LA "OUTPUT-OBSERVABILIDAD"

Observación 2

Es obvio que si la matriz T_ℓ (consecuentemente M_ℓ) tiene rango máximo por filas para algún $\ell \in \mathbf{N}$ entonces todas las matrices T_j (consecuentemente M_j) con $j \le \ell$ tiene rango máximo por filas.

Además se tiene la siguiente proposición.

Proposición 4

Sea (A,B,C,D) *un sistema. Para todo* $\ell \ge n$ *tenemos que*

$$\operatorname{rango} T_{\ell+1} - \operatorname{rango} T_\ell = \operatorname{rango} T_{\ell+2} - \operatorname{rango} T_{\ell+1}$$

Demostración:

Sea (A,B,C,D) un sistema, teniendo en cuenta la proposición 2 y el corolario 2, podemos considerar un sistema equivalente en la forma (A_1,B_1,C_1,D_1) con

$$A_1 = \begin{pmatrix} 0 & \bar A_1\\ 0 & \bar A_2\end{pmatrix},\ B_1 = \begin{pmatrix} \bar B_1 & 0\\ \bar B_2 & 0\end{pmatrix},$$

$$C_1 = \begin{pmatrix} I_c & 0\\ 0 & 0\\ 0 & 0\end{pmatrix},\ D_1 = \begin{pmatrix} 0 & 0\\ 0 & 0\\ 0 & I_d\end{pmatrix}$$

Con $\bar A_2 \in M_{\delta-c}(\mathbb{F})$.

En el caso en que $d = p$ la matriz $C_1 = 0$ por lo que el resultado es obvio,

En el caso en que $d = k$ la matriz $B_1 = 0$. Llamando

$$\bar C = \begin{pmatrix} I_c & 0\\ 0 & 0\end{pmatrix}$$

y teniendo en cuenta que $A^\delta = \sum_{i=0}^{\delta-1} A^i$, tenemos

$$
\operatorname{rango}\begin{pmatrix}
\bar C & & & & & & \\
0 & I_d & & & & & \\
\bar C A & 0 & 0 & & & & \\
0 & 0 & I_d & & & & \\
\vdots & & \ddots & & & & \\
CA^{\delta-1} & 0 & 0 & 0 & \ddots & 0 & \\
0 & 0 & 0 & 0 & \ddots & I_d & \\
0 & 0 & 0 & 0 & \ddots & & 0\\
0 & 0 & 0 & 0 & \ddots & & I_d\\
\vdots & & & & & &
\end{pmatrix}.
$$

Entonces,

$$\operatorname{rango} T_{\ell+1} - \operatorname{rango} T_\ell = d,\ \forall \ell \ge \delta.$$

Supongamos ahora, $d \ne p,k$. Primeramente, analizamos el caso particular donde $\bar A_1 = 0$.

Teniendo en cuenta la forma triangular por bloques de las matrices T_ℓ es fácil observar que

$$\operatorname{rango} T_{\ell+1} - \operatorname{rango} T_\ell = \operatorname{rango} \bar B_1 + d.$$

Observamos que este caso incluye otro caso particular donde $c = \delta$ y entonces $A_1 = 0$.

Entonces, analizamos el caso $\bar A_1 \ne 0$. Tenemos

$$
\operatorname{rango} T_\ell =
\begin{pmatrix}
I_r &&&&&&& \\
& I_d &&&&&& \\
&& \ddots &&&&& \\
&&& I_d &&&& \\
&&&& \bar{A}_1 & \bar{B}_1 && \\
&&&& \bar{A}_1\bar{A}_2 & \bar{A}_1\bar{B}_2 & \bar{B}_1 & \\
&&&& \vdots && \ddots & \\
&&&& \bar{A}_1\bar{A}_2^{\ell} & \bar{A}_1\bar{A}_2^{\ell-1} & \dots & \bar{A}_1\bar{B}_2 \quad \bar{B}_1
\end{pmatrix}
$$

Consideremos ahora, la siguiente reducción de orden del sistema $(\bar{A}_2, \bar{B}_2, \bar{A}_1, \bar{B}_1)$ y aplicamos los pasos previos.

Corolario 3

Sea (A, B, C, D) un sistema. Para todo $\ell \geq n$tenemos que

$$\operatorname{rango} M_{\ell+1} - \operatorname{rango} M_\ell = \operatorname{rango} M_{\ell+2} - \operatorname{rango} M_{\ell+1}$$

Como corolario, y teniendo en cuenta la observación 2, podemos concluir el siguiente resultado.

Teorema 2

Un sistema (A, B, C, D) es "output-observable" si y sólo si la matriz $M_\delta$tiene rango máximo por filas.

Este teorema proporciona un método iterativo para conocer el carácter de "output-observabilidad" del sistema.

Algoritmo:

Paso 1: Calcular $\operatorname{rango} M_0$. Si $\operatorname{rango} < p + \delta$ el sistema no es "output-observable",

Si $\operatorname{rango} = p + \delta$, entonces

Paso 2: Calcular $\operatorname{rango} M_\ell$. Si $\operatorname{rango} < (\ell+1)p + (\ell+1)\delta$ el sistema no es "output-observable".

Si $\operatorname{rango} = (\ell+1)p + (\ell+1)\delta$ y $\ell = \delta$ el sistema es "output-observable", y si $\ell < \delta$ volver al paso 2.

V. Conclusiones

En este artículo se presenta un examen detallado de la estructura algebraica de los códigos convolucionales empleando técnicas de la teoría de sistemas lineales. La propiedad de "output-observabilidad" se ha analizado y se han obtenido condiciones para asegurar esta propiedad. Finalmente, se presenta un algoritmo para evaluar la "output-observabilidad".

Bibliografía

[1] J.J. Climent, V. Herranz, C. Perea, A first approximation of concatenated convolutional codes from linear systems theory viewpoint. *Linear Algebra and its Applications* vol. 425, pp. 673-699, (2007).

[2] J-J. Climent, V. Herranz, C. Perea, Linear system modelization of concatenated block and convolutional codes, *Linear Algebra and its Applications*, vol. 429, pp. 1191-1212, (2008).

[3] A.Díaz, M.I.García-Planas, An alternative collection of structural invariants for matrix pencils under strict equivalence}, *Wseas Transactions on Systems and Control,* vol. 4, (10), pp 487-496, (2009).

[4] J.L. Domínguez, M.I. Garcia-Planas, B. Mediano, Input Observability Analysis of Fixed Speed WindTurbine *Mathematical Modelling and Simulation in Applied Sciences*. Wseas Press, pp. 13-19, (2012).

[5] P.Elias, Coding for Noisy Channels, IRE Conv.Rec. vol. 4, pp. 37-46, (1955).

[6] Ch.Fragouli, R.D. Wesel, Convolutional Codes and Matrix Control Theory, *Proceedings of the 7th International Conference on Advances in Communications and Control*, Athens, Greece, (1999).

[7] G.D. Forney, Convolutional codes: Algebraic structure. *IEEE trans. Information Theory*, (1970).

[8] M.I. García-Planas, Sensivity and stability of singular systems under proportional and derivative feedback}, *Wseas Transactions on Mathematics*, vol. 8, (11), pp 635-644, (2009).

[9] M.I. García-Planas, Bifurcation diagrams of generic families of singular systems under proportional and derivative feedback. *Wseas Transactions on Mathematics*, vol. 7, (2), 1-11, (2008).

[10] M. I. García-Planas, El M. Souidi, L.E. Um, Convolutional codes under linear systems point of view. Analysis ofoutput-controllability. *Wseas Transactions on Mathematics*. vol 11 (4), (2010), pp. 324-333.

[11] H. Gluesing-Luerssen, U.Helmke, J.I. Iglesias Curto Algebraic Decoding for Doubly Cyclic Convolutional Codes, *Advances in Mathematics of Communications* vol. 4, pp. 83-99, (2010).

[12] R.Hutchinson, J.Rosenthal,R.~Smarandache, Convolutional codes with maximum distance profile, *Systems Control Lett*. Vol. 54 (1), pp- 53-63, (2005).

[13] J.I. Iglesias, A study on convolutional Codes. Classification, new families and decoding, Tesis Doctoral, (2007).

[14] M.Kuijper, R.Pinto, On minimality of convolutional ring encoders. *IEEE Trans. on Information Theory*, vol. 55, (11), pp. 4890-4897, (2009).

[15] H.Loeliger, G.~D.Forney, T. Mittelholzer, M.D. Trot, Minimality and observability of group systems, *Linear Algebra and its Applications*, vol. 205-206, pp. 937-963, (1994).

[16] J.L.Massey, M.K.Sain, Codes, Automata and continuous systems: explicit interconnections. *IEEE Trans. on Automatic Contro*l, Vol AC-12 (6), pp. 644-650, (1967).

[17] J.Rosenthal, Some interesting problems in systems theory wich are of fundamental importance in coding theory, *Proceedings of the 36th IEEE Conference on Decision and Control*, (1997).

[18] J.Rosenthal, An algebraic decoding algorithm for convolutional codes. In G. Picci and D. S. Gilliam, editors, *Dynamical Systems, Control, Coding, Computer Vision; New Trends,*

[19] *Interfaces, and Interplay,* pp. 343-360. Birkh\"auser, Basel, (1999).

[20] J.Rosenthal, E.V.York, BCH Convolutional Codes, *IEEE Trans. Information Theory* vol. 45 (6), 1833-1844, (1999).

[21] J.Rosenthal, J.M.Schumacher, E.V.York, On Behaviors and Convolutional Codes, *IEEE Trans. on Information Theory*, vol. 42, (6), pp. 1881-1891, (1996).

[22] E. Zerz, On multidimensional convolutional codes and controllability properties of multidimensional systems over finite rings. *Asian Journal of Control*, vol. 12, (2), pp. 119 126, (2010).